

DIGITAL BUSINESS TECHNOLOGIES: E-COMMERCE AND VIRTUAL TRADE

Ковтонюк К. В., к.е.н., доцент

*Київський національний економічний університет
імені Вадима Гетьмана
м. Київ, Україна*

Молчанова Е. Ю., к.е.н., доцент

*Київський національний торговельно-економічний університет
м. Київ, Україна*

DOI: <https://doi.org/10.30525/978-9934-26-028-5-14>

ТОРГОВЕЛЬНІ БАР'ЄРИ В УМОВАХ ДІДЖИТАЛ-ЕКОНОМІКИ

Діджитал-торгівля виникла завдяки новим стимулюючим технологіям, для яких торговельні обмеження ще не мали можливості розвиватися, а необхідність лібералізації такої торгівлі стає меншою. У той же час нові технології піднімають нові проблеми торговельної політики, в тому числі відсутність загальних правил та принципів, які допомагають регулювати таку торгівлю, поява нових торгових бар'єрів і більш широкі питання державної політики щодо онлайн інформації [1]. Частково, це відбиває вплив цифрової трансформації на здатність урядів здійснювати внутрішню політику регулювання [2], в тому числі в таких областях, як конфіденційність і кібербезпека.

Торговельні бар'єри в умовах діджитал-економіки визначаються Управлінням торгового представника США (USTR) як обмеження або практики, що впливають на транскордонні потоки даних, діджитал-продукти, послуги з підтримкою Інтернету та інші обмежувальні вимоги до технології. Тож розглянемо класифікацію бар'єрів діджитал-торгівлі зі сторони уряду і бізнесу (табл. 1). Перші чотири категорії включають нові бар'єри, характерні для діджитал-сфери. Інші чотири категорії бар'єрів

стосуються більше «реальної» сфери. Права на інтелектуальну власність є наскрізними питаннями у всіх режимах.

Таблиця 1

Класифікація бар'єрів діджитал-торгівлі [3]

Категорія бар'єру	Можливі бар'єри
1	2
1. Можливі проблеми в сприятливом середовищі	<ul style="list-style-type: none"> - доступ до вмісту (пропускна здатність, цензура та фільтрація веб-контенту); - політика даних (вимоги щодо конфіденційності даних, збереження даних, особисте право на конфіденційність даних, санкції за недотримання); - обмеження щодо онлайн-продажів та транзакцій; - виключення іноземних фірм від участі на місцевих ринках; - нерациональне застосування старих регуляторних режимів до нових бізнес-моделей; - обмеження щодо реклами в Інтернеті.
2. Технічні обмеження торгівлі	<ul style="list-style-type: none"> - політика даних (обмеження транскордонних потоків даних); - стандарти (шифрування, сертифікація безпеки продукту тощо); - операції в Інтернеті (бар'єри на шляху до виконання, реєстрація доменних імен (DNS), продажі в Інтернеті); - обмеження способів оплати, онлайн-ліцензування платежів тощо; - обтяжлива практика електронних підписів та автентифікація; - національні стандарти та обтяжлива оцінка відповідності.
3. Техно-логічні бар'єри	<ul style="list-style-type: none"> - кібер-стандарти: недостатній захист та невідповідність міжнародній практиці; - ризики кібербезпеки (надмірне шифрування, доступ до зашифрованих даних); - вимога щодо здачі патентів, вихідних кодів, комерційних тасмниць; - вимоги до розкриття алгоритмів шифрування.
4. Вимоги до локалізації даних	<ul style="list-style-type: none"> - вимоги до побудови локальної серверної інфраструктури; - політика даних щодо конфіденційності тощо, яка потребує зберігання на локальних серверах; - заборона транскордонних потоків даних.

1	2
5. Права на інтелектуальну власність	<ul style="list-style-type: none"> - порушення прав інтелектуальної власності (авторські права, патент, комерційна таємниця); - недостатній захист авторських прав, патентів та комерційних таємниць; - програмне піратство; - обхід технологічного захисту.
6. Обмеження щодо заснування	<ul style="list-style-type: none"> - конкурентна політика; - мобільність бізнесу (квоти, обмеження часу перебування); - вимоги до партнерства з місцевими компаніями; - обмеження ради директорів та управління.
7. Фіскальні обмеження	<ul style="list-style-type: none"> - оподаткування та субсидії; - митні збори на «електронні передачі»; - тарифи на продукти ІКТ та на товари, що мають важливе значення для цифрового сектору, такі як напівпровідники, ІКТ обладнання, електронні інтегральні мікросхеми тощо.
8. Державні підприємства	<ul style="list-style-type: none"> - державні закупівлі (пільгові схеми закупівель діджитал-продуктів та послуг); - обмеження участі іноземних держав у тендерах (телекомунікації, забезпечення програмним забезпеченням); - недобросовісна конкуренція державних підприємств; - місцеві вимоги до змісту як умова укладання договорів державних закупівель.

В останньому випадку ми бачимо, що комерційні підходи у «реальній» сфері є досить актуальними: там, де компанії раніше робили капітальні вкладення для залучення проектів та споживачів, в діджитал-сфері вони, ймовірно, будуть пропонувати низькі ставки на проекти для отримання доступу до даних для їх капіталізації. Заява китайської фірми Baidu про те, що вона випустить своє програмне забезпечення для автомобілів з автоматичним управлінням в обмін на отримані дані є прикладом цієї форми.

Протекціоністська політика країн може встановити бар'єри для діджитал-торгівлі або зменшити довіру до діджитал-економіки в цілому, що в свою чергу може призвести до фрагментації (поділу) Інтернету або дискримінаційного

торговельного поводження. Пропонуємо розглянути потенційні перешкоди діджитал-торгівлі, які можуть виникнути [4]:

1. Суверенітет Інтернету. У деяких країнах уряд шукає суворого контролю над діджитал-даними в межах своїх кордонів та визначає, до якої інформації люди можуть отримати доступ в Інтернеті та як ділитися інформацією всередині та за її межами, створюючи цифрові торговельні бар'єри. Наприклад, фірми, що працюють в Китаї, відчувають різні перешкоди, такі як цензура (так званий «Золотий щит»), вимоги щодо місцевих стандартів та перевірки національної безпеки; російські закони забороняють віртуальні приватні мережі та вимагають від постачальників послуг зашифрованого обміну повідомленнями.

2. Локалізація та транскордонні обмеження потоку даних. Політика локалізації даних включає в себе веб-фільтрацію та блокування, митні тарифи на цифрові продукти, вимоги до розкриття вихідного коду тощо. Закони про локалізацію даних часто вимагають від іноземних компаній зберігання даних на локальних серверах. Загалом, локалізація даних включає всі політики, які перешкоджають передачі даних, наприклад, змушуючи компанії обробляти дані локально або вимагати індивідуального чи урядового дозволу перед передачею даних. Ці види політики обмежують потік даних та збільшують витрати для іноземних компаній, що конкурують на місцевих ринках, змушуючи їх витратити більше на додаткові технологічні рішення, зберігання даних та інші послуги. Організації домагаються ефективного доступу до ринку шляхом вільного переміщення даних через національні кордони або за допомогою хмарних сервісів. Опитування, проведене USITC в 2017 році, показало, що локалізація даних – це найбільш поширений політичний захід, який перешкоджає діджитал-торгівлі. Наприклад, регламент Європейського Союзу щодо захисту даних встановлює обмеження щодо використання та транскордонної передачі особистих даних осіб [5].

3. Кібер-крадіжка або примусовий трансфер технологій. Порушення прав інтелектуальної власності (ІВ) або відсутність

застосування права інтелектуальної власності можуть обмежувати можливість компанії в повній мірі отримати переваги від її інновацій та інвестицій, таких як комерційна таємниця, фірмові алгоритми або вихідний код. Порушення прав інтелектуальної власності в діджитал-середовищі особливо важко оцінити, але це вважається значним показником, що потенційно перевищує обсяг продажів за допомогою традиційних ринків або законних завантажень.

4. Нормативні питання. Уряди можуть пред'являти вимоги, які фірми вважають занадто обтяжливими, тим самим сприяючи розвитку місцевих фірм. Регламенти можуть застосовуватися, наприклад, дискримінаційно або надмірно обмежуючи торгівлю, створюючи торгові бар'єри для іноземних фірм. Наприклад, в Індії є обов'язковою реєстрація всього імпорту товарів ІКТ у національному агентстві зі стандартизації.

Отже, широке розповсюдження торговельних бар'єрів для діджитал-товарів та послуг призвело до підвищеної уваги до цієї теми. Це спричинило необхідність включення до структури торговельних угод про вільну торгівлю розділів про діджиталізацію. Слід зазначити, що подібні практики/кейси мали місце в комплексній та прогресивній угоді про Транс-Тихоокеанське партнерство (СРТПП) і угоди США-Мексика-Канада (USMCA). Ці угоди захищають вільний потік інформації через кордон, забороняючи локалізацію даних, обов'язкове розкриття вихідного коду та мита на діджитал-продукти.

Члени СОТ погодилися не вводити митні збори за електронні передачі. Хоча діджитал-торгівля охоплена Генеральною угодою про торгівлю послугами (GATS), конкретні проблеми діджиталізації, такі як локалізація даних та примусова передача технології, не розглядаються. У січні 2019 року 76 членів СОТ – включаючи США, ЄС та Китай – заявили про намір розпочати переговори щодо зняття бар'єрів у діджитал-торгівлі. Успішне завершення цього процесу допомогло б упорядкувати зусилля для подолання торгових бар'єрів діджиталізації, таких як локалізація даних у глобальному масштабі.

Література:

1. Cory Nigel. Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? *Information Technology & Innovation Foundation*. 2017. URL: <https://cutt.ly/7jDQpDi>.
2. Aaronson Susan Ariel. Solutions to the digital trade imbalance. *VOX_{EU}*. 2016. March 07. URL: <https://cutt.ly/tjDQ8gG>.
3. Ciuriak Dan, Maria Ptashkina. The Digital Transformation and the Transformation of International Trade. RTA Exchange, Issue paper. 2018. URL: <https://cutt.ly/0jDQheX>.
4. Digital Trade (2019). Congressional Research Service (CRS). 2019. March 29. URL: <https://crsreports.congress.gov>.
5. Lauren Kyger “Data Localization” And Other Barriers To Digital Trade. *Trade Vistas*. 2019. February 21. URL: <https://cutt.ly/HjDQdv4>.